UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

OCT 27 2017

MEMORANDUM

SUBJECT: Response: EPA Has Not Initiated Required Background Investigations for Information Systems Contractor Personnel Report No. 17-P-0409

FROM: Steven Fine, Office of Environmental Information (OEI)

Donna J. Vizian, Office of Administration and Resource Management (OARM)

TO: Arthur A. Elkins Jr.

Thank you for the opportunity to respond to the issues and recommendation in the subject audit report. Following is a summary of the Agency's overall position as well as a description of the already implemented or intended corrective actions.

The Agency agrees with the Office of Inspector General recommendation that the Agency implement controls over the EPA's personnel screening practices for initiating the required high-level background investigations for contractor personnel with privileged access to federal networks.

The Environmental Protection Agency (EPA) has already implemented controls to verify screening practices for initiating the appropriate level of background investigation through two separate processes that ensure that no-one is issued a Privileged User Card (PUC) without having at least a Tier 4 background investigation and an Active Directory (AD) account with elevated privileges.

While the Position Risk Designation Checklist (EPA Form 1480-95) is not currently part of the non-federal risk designation process, the EPA does have a process in place to risk designate non-federal employees. The non-federal risk designation process has a built-in control specific to those who require privileged access rights to federal IT systems. The first control occurs prior to onboarding, when the Contracting Officer's Representative (COR) is prompted to respond to 7 questions pertaining to each non-federal position. The current risk designation process for non-federal personnel includes a specific question about IT access. If the response is affirmative, the designation is automatically established as "High Risk."

The link below explains to CORs how to respond to the Office of Administration Services Information System (OASIS) EPA Personnel Access and Security System (EPASS) designation questions. While the response to question number 7 currently includes several examples of titles that might necessitate elevated access rights, OARM will adding position titles to the examples to make them more comprehensive, per the OIG's observation. OARM expects to complete this by the end of October, 2017. Expanding the list of titles will clarify the positions that will lead to an affirmative response. The CORs' user guide explains each of the questions and provides examples of position titles that would drive an affirmative response for the question. The guide can be found at http://intranet.epa.gov/oa/smd/pdfs/risk-designation-for-non-epa-personnel-questionsandguidance.pdf. The question related to privileged access is:

Q7) Does the position have administrative rights to the EPA network or systems within the network? Or does the position require elevated access to EPA's network/systems?

The second review takes place when the PUC is requested. The eBusiness request initiates a process that requires approval of an Active Directory (AD) account by the IMO. OARM receives the request and approval, and confirms that the person has the appropriate Tier 4 background investigation (BI) in place. Approval to print the PUC is only provided when (at a minimum) the Tier 4 is initiated and the Active Directory (AD) account has been established (which requires the IMO approval). Attached is the process flow, which shows that a new recipient would need both an AD account established and a Tier 4 BI initiated before the approval to print the PUC is given. The result of the new approvals is that no PUC has been issued without a Tier 4 investigation having been initiated since April 27, 2017.

Additionally, EPA has begun to communicate among agency personnel concerning the need to verify the appropriate background investigation level for contractors with privileged access. The first communication was sent on October 12, 2017 (see attached) and was sent to all Assistant Regional Administrators, all Program Management Officers and all Human Resource Officials. This information is also being provided in the OEI/OCFO/OARM Administrative Update to First Line Supervisor's nationwide. Also, the Chief Information Security Officer (CISO) has briefed the agency Information Security Officers and Information Management Officers.
Lastly, regarding data accuracy, the OARM's PUC dashboard, tracks the background investigation process and status for all PUCs. OEI and OARM agree that the PUC dashboard is the authoritative source of PUC information for the Agency. OEI and OARM also concur that the data in the PUC dashboard is accurate.

If you have any questions related to responses to the Management Alert: EPA Has Not Initiated Required Background Investigations for Information Systems Contractor Personnel, please contact Jeffrey Anouilh anouilh.jeffrey@epa.gov in OEI or Kelly Glazier glazier.kelly@epa.gov in OARM.